Advanced Subscriber Identity Privacy in 3GPP Mobile Systems

Kshitij Ajagaonkar, Akshay Bhalerao, Shahajan Fakir, Vinayak Jagdale, Durga Phadatare

[1]*Kshitij Ajagaonkar, Dept., Computer Science and Engineering, Sanjay Ghodawat Institute, Maharashtra, India*
[2]*Akshay bhalerao, Dept., Computer Science and Engineering, Sanjay Ghodawat Institute, Maharashtra, India*
[3]*Shahajan Fakir, Dept., Computer Science and Engineering, Sanjay Ghodawat Institute, Maharashtra, India*
[4]*Vinayak Jagdale, Dept., Computer Science and Engineering, Sanjay Ghodawat Institute, Maharashtra, India*
[5]*Durga Phadatare, Dept., Computer Science and Engineering, Sanjay Ghodawat Institute, Maharashtra, India*

---***---

Abstract - *Evolution in Cellular networks starting with 1G, followed by 2G and then by 3G, cellular networks have progressed rapidly. A recent technology that has marked the beginning of 4G is Long Term Evolution (LTE). With transmission technologies, mechanisms for authentication, confidentiality protection, etc., improved appreciably through the generations, not much improved with regards to the subscriber's identity privacy, and there is absence of exception in LTE. Much of this could be due to the trust model implemented in these networks. Introduction of responsive services like mobile-banking, mobile commerce, etc., has grown bigger the importance of identity privacy. Identification of threats like tracking the location and comprehensive profiling where data about movement, usage, etc., of a subscriber is collective and linked to person's identity to explore various attacks is quite shocking. In this paper, new trust model has been tried for strengthening identity privacy in cellular networks; it has an additional capacity to achieve better interoperability among different cellular operators. A security extension has been proposed to adopt this trust model as to improve the identity privacy in LTE as well as the interoperability. A formal analysis of the extension proves that it fulfill its security goals.*

***Key Words*: Cellular networks, Trust model, Long Term Evolution(LTE), Authentication and Key Agreement, Identity privacy, NS 2.3x.**

1.INTRODUCTION *(Size 11 , cambria font)*

Wireless network is a computer network that is wireless, and it is commonly associated with a telecommunications network. In this network interconnections between nodes are implemented without any use of wires. Wireless telecommunications networks are implemented with some type of remote data transmission system that uses electromagnetic waves, such as radio waves, for the carrier. Usually this implementation takes place at the physical level or "layer" of the network.

The purpose for using wireless network are cost-effectiveness for deployment of network, and its applicability to environments where use of wires is not possible or it is favored solution as compared to wired networks. Software simulation tools are often used for designing wireless networks, also studying their behavior under various conditions,

A common basic architectural framework is used in all cellular networks. In this basic architecture three parties are involved. They are as follows the User Equipment (UE), the Home Network (HN) and a Serving Network (SN). The UE that a subscriber owns is registered with the HN. When the subscriber procures a Subscriber Identity module (SIM) from the HN and fits it into his/her UE at that time the association between the UE and the HN is get created. The HN offers services to its registered User Equipment's through Serving Networks that are located within or outside its own service area.

The radio link is used for the communication between UE and SN. The wired medium is used for communication between the SN and the HN. The radio link is too open by nature for comfort of challenger so it is vulnerable to various kinds of attacks. So the wired link is secured compare to radio link.

The unique permanent identity called International Mobile Subscriber Identity (IMSI) is assigned by the HN [3] to the user equipment (UE). The purpose of providing this unique identity to the each and every user is for unique identification of a subscriber for authentication, authorization and billing purposes. The IMSI is valuable information. This IMSI should not be accessible to anyone. It should be accessible to HN. Its compromise will expose the subscriber to threats like location tracking as well as comprehensive profiling (i.e. data about movement, usage, etc.), of a subscriber is collect and linked to user's identity to explore different attacks at a later time.

The UE needs to go through an Authentication and Key Agreement (AKA) procedure to access a particular service. The UE has to send an identity with a service request to the SN during an AKA, The SN obtains relevant authentication data from the HN by presenting the identity that it received from the UE.

The UE authenticated with the help of a challenge response mechanism. In the current trust model there are occasions during identity presentation in the AKA procedure, when the IMSI needs to be transmitted to the SN in clear text through the vulnerable radio path.

The current trust model needs the SNs to be considered trustworthy, undermining the threat that a compromised third party SN may pose. Such requirement demands unconditional trust. And also limits interoperability.

2. CURRENT TRUST MODEL

In the trust model, which is current, the included trust requirements with reference to the permanent identity of a subscriber existed

 HN: As the UE is registered and has a direct service agreement with the HN; it is bound to fully trust the HN with its IMSI.HN

 SN: Since HN serves its subscribers through SNs; the HN confers full trust in the SN with regards to the IMSI of a subscriber. For authentication, authorization and billing purposes, the IMSI is exchanged unabated between the HN which is home network and the SN which is service network. UE

 SN: It is a transitive relation which is outcome of the previous two trust relations; because of which, the UE fully trusts the SN with its IMSI and it transmits its IMSI immediately upon receiving a request sent by SN. By the trust requirements given above, one can easily understand that even though the SN may belong to an entrusted third party cellular operator, the UE and the HN is required to confer unconditional trust on it.

As a result, there exist several vulnerabilities, which an adversary may explore to compromise identity privacy of the subscriber. Moreover, such trust requirements are impractical in today's context when to provide high coverage to the customer; multiple cellular operators have to get united. The common practice is to do roaming agreements to provide service in a region when the third party operator has not set up its foundation over there. The times need is to shift the standard prototype that will look at the trust issues from the different aspect an aspect that gives more emphasis on issues like privacy and interoperability.

3. PROPOSED TRUST MODEL

In this section, a new trust model is proposed that is more flexible compared to the currently adopted trust model of cellular networks. The only trust requirement is there
Which is as follows:

UE HN: The UE will not trust anything else than its registered HN. The IMSI should not be shared with any third party and in any situation should not leave the UE or the HN. The above trust model will strengthen identity privacy, as the IMSI will get shared to only with HN and no one else. It will also improve interoperability among cellular operators, since the requirement to believe the SN related to the persistent identity is totally relaxed. In order to adopt this model to provide advanced confidential identity, an alternate contrivance for identity presentation, this can be used in all situations when an IMSI is used or else to be composed.

To approve this model even with respect to confidentiality and integrity assurance of user data, two end ciphering and integrity, which is application layer based, protection solutions like IPsec can be used. [11] With cellular networks gradually moving towards all-IP, such solutions will not be too hard to implement

4. SECURITY ARCHITECTURE OF LET

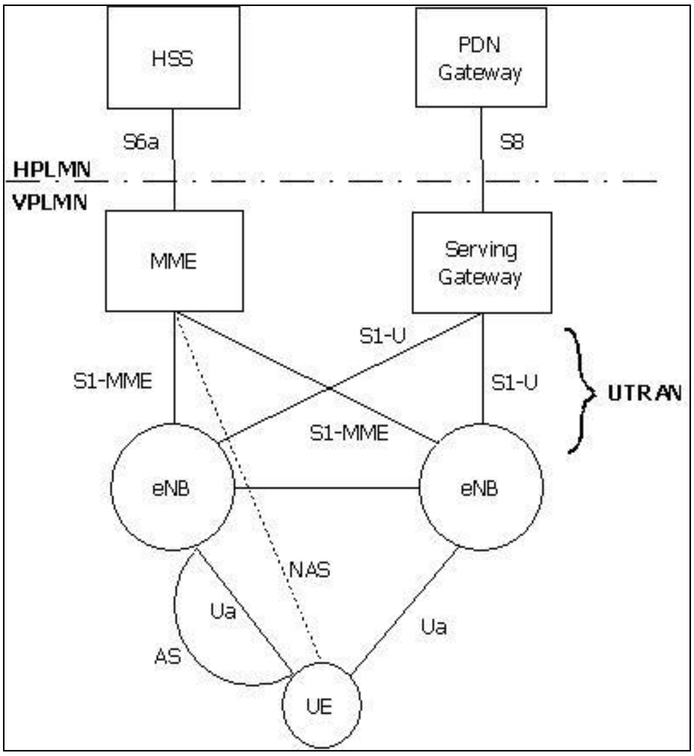

Fig -1: Simplified Architecture of LTE.

Fig. 1 depicts a simplified view of the roaming security architecture of an Evolved Universal Terrestrial Radio Access Network (E-UTRAN) [3] that serves as the core of LTE. In this, shows only the key elements associated with the AKA procedure used in LTE. Each and every user is registered with a Home public Land Mobile Network (HPLMN) (which, is the HN of the user) with their subscription and profile information stored in a Home Subscriber Server (HSS).

In the Visiting Public Land Mobile Network (VPLM) (which, is the SN of the user), the User Equipment (UE) connects with an evolved EnodeB (eNB) through the Uu interface, for attach, Tracking Area Update (TAU) and service requests. ENB is the new enhanced Base Transceiver Station (BTS) that provides the LTE air interface and performs radio resource management for the evolved access system. An eNB is hooked up with single or more Mobility Management Entities (MME) through the S1-MME interface. For the LTE access network and for authenticating the user by

interacting with the HSS, the MME is being used as a key control node.
For obtaining data of authentication, the S6a interface will be used for communication between the MME and the HSS. Between the UE and the E-UTRAN, there are two layers of security. The initial layer is the Access Stratum (AS) which protects the Radio Resource Control (RRC) plane signaling and also the User Plane (UP) data between the UE and the eNB. The second layer is called the Non Access Stratum (NAS) which secures the control plane signaling between the UE and the MME. Through the Packet Data Network Gateway (PDNGW), UE has access to packet data, via the Serving Gateway (SGW).

5. EPS-AKA

The AKA procedure used in LTE which is EPS-AKA [2], it creates keying material figuring a basis for UP, RRC, and NAS ciphering keys as well as RRC and NAS integrity securing keys. During the initial connection and successive connections EPS-AKA are as follows:

5.1 The Initial Connection

For the initial connection (when the subscriber switches on the UE for the first time), the attach request is being transferred by the UE to the MME. In the consideration of the UE does not have a temporary identity at this moment, its IMSI is constituted in this request. During the initial connection, the EPS-AKA procedure is as follows:

(1) The MME calls forth the agenda by requesting authentication data from the HSS. The request shall include the IMSI and the SN/MME identity.

(2) The HSS accumulates a Universal Mobile Telecommunication System - Authentication Vector (UMTS-AV), upon the request receipt. An UMTS-AV contains a random part RAND, an authenticator token AUTN used for authenticating the network to the UE, an expected response XRES, and a 128-bit Cipher Key CK, a 128-bit Integrity Key IK.

UMTS-AV= (RAND; AUTN; XRES; CK; IK) (1)

The AUTN having a sequence number SQN used to describe freshness of the AV. By replacing CK and IK with a Key for Access Security Management Entity (KASME), an EPS-AV is then derived from UMTS-AV.

To derive KASME, a Key Derivation Function which is KDF [2] is used. It will use the input parameters: CK, IK and SN/MME Identity. Thus,

KASME = KDF (CK; IK; MME-identity) (2)

EPSAV= (RAND; AUTN; XRES; KASME) (3)

The HSS then sends EPS-AV back to the MME.

(3) The MME extracts RAND and AUTN from EPS-AV after receiving it.and sends them to the UE as a challenge. A Key Set Identifier (KSIASME) has been come with the Challenge. The KSIASME will be used to make it possible for the UE and the MME to identify a KASME without invoking the authentication procedure. This is used to allow reuse of the KASME during subsequent connections.

(4) At receipt of this message, the UE runs UMTS algorithm [1] to verify that AUTN is correct and hereby the network is being authenticated. The UE will reject the authentication, if AUTN is incorrect..

If AUTN is correct, the UE computes RES, IK and CK (using UMTS algorithm). It then derives the KASME from the newly computed IK and CK. The UE will send a user authentication response back to the MME message that having the computed RES.

(5) Finally, MME checks whether RES is equal to XRES. If so, the authentication is successful. If it is unsuccessful, an authentication reject message will be sent towards the UE by the MME. A KASME is shared between UE and MME at the end of a successful EPS-AKA. A hierarchy of keys are then generated from the KASME to be used for protection of the NAS and the AS. By initiating a GUTI reallocation procedure through the NAS, the MME then allocates a fresh temporary identifier called Globally Unique Temporary Identity (GUTI) [4] to the UE.

The MME sends GUTI Reallocation Command to the UE and the UE returns GUTI Reallocation Complete message to the MME during the GUTI reallocation procedure. A new GUTI shall be sent to the UE only after a successful activation of NAS security. A mapping between the GUTI and the IMSI of the UE is maintained at the MME. the GUTI will give an apparent identification of the UE, because of that the subscriber's permanent identity (i.e., the IMSI) is not revealed. Entire part is considered with reference.

5.2 Subsequent Connections

For subsequent connections (during attach requests, Tracking Area Updates (TAU) and service requests), identity presentation of the UE is accomplished by transmitting a GUTI through the radio path. The KSIASME is also sent along with the request. Before transmitting, the UE integrity protects the request using NAS security. Upon receipt of the connection request, the MME identifies the corresponding KASME with the help of the received GUTI and the KSIASME. The MME then checks the integrity protection of the message. If the integrity check succeeds, the MME, depending on the MME policy, may either decide to reuse KASME that was established during a previous AKA (without invoking a fresh authentication procedure) or may decide to go for a fresh EPS-AKA that will result in the establishment of a new KASME.

In order to carry out a fresh EPS-AKA, the MME locates the IMSI of the UE in its local database through the IMSI-GUTI mapping and continues in the same manner as the initial connection (discussed above). In order to reuse a KASME a fresh set of keying material is derived from the KASME. Thus, the need to perform frequent AKA runs has been reduced in EPS through the use of a more elaborate key hierarchy. In particular, connection requests can be authenticated using a stored KASME without the need to perform a fresh AKA. Several successive connections may be secured through re-derived security contexts from the current KASME. Entire part is considered with reference

6. SECURITY EXTENSION FOR EPS-AKA

In this section, a security extension for EPS- AKA is proposed to achieve improved identity privacy and enhanced interoperability in LTE. The extension protects the permanent identity of a sub-scriber in the radio path as well as in the wired path. Knowledge of the IMSI of a subscriber is restricted only to the UE and the HE. In the extension, a Dynamic Mobile Subscriber Identity (DMSI) is transmitted by the UE instead of the IMSI. The role of the DMSI is to randomize and mask the IMSI so that an adversary having access to a particular DMSI cannot link it with any subscriber or any previous communication. This extension is based on our work that was presented in [5]. For successful functioning of the security extension the following operator specific random number and functions are used:

RIC: Random number for Identity Confidentiality (RIC) is a random number that uniquely identifies a UE within a particular HE for an epoch of time. RIC is used to compute a DMSI as

DMSI = MCC||MNC||RIC||ERIC (4)

Where, MNC, MCC and ERIC stands for Mobile Network Code, Mobile Country Code and Encrypted RIC respectively. Size of RIC (b) in bit should be lesser than 128 bits and shall be determined by the operator depending on the subscriber base of the HE. A RIC of size b provides a pool of n = 2b unique RIC values. A fresh not-in-use RIC called RICFresh is chosen every time a new EPS-AV is generated at HSS.

RICFresh is then cryptographically embedded into the RAND of EPS-AV. The resultant random number after embedding RIC into RAND is called Embedded RAND (ERAND). Only UE having the knowledge of the long term shared key Ki is capable of extracting RIC from the ERAND.Multiple (m) RICs comprising of the fresh and few previously generated RICs; RICNew; RICPrev; RICOld etc. Are maintained at the HSS against a particular IMSI in order to ensure robustness of the protocol even when an AV gets lost in transit (or due to some reason does not get utilized). Such an arrangement ensures that a mapping between the RIC that is currently stored at the UE and the corresponding IMSI is always maintained at the HSS. An additional RIC called RIC in Use is maintained at the HSS. RIC in Use enables the MME to uniquely identify the UE as long as the later continue to stay within the former's service area.

Fi: This function returns a RIC that can be used to uniquely identify an UE. This is done by randomly selecting a not-in use RIC from the RIC-Index, the latter being an index for the HSS's

Local database consisting of n = 2b unique RIC entries arranged in ascending order (Fig. 2), b being the number of bits in RIC. Each RIC entry in the RIC-Index has a pointer called IMSI- Pointer against it. A RIC that is already allotted to some UE, will have its IMSI-pointer pointing to that particular row in the HSS's database, which contains the IMSI of the concerned UE. A null pointer against a particular RIC in the RIC-Index denotes that the particular RIC is (not-in-use) not allotted to any specific UE and is free to be used.

RIC = fi (RIC-Index) (5)

Fe: This function embeds RIC into RAND to produce ERAND, using the long term shared secret key Ki as parameter.

ERAND = feKi (RIC; RAND) (6)

FX: This function extracts RIC from ERAND, using the long term shared secret key Ki as parameter.

RIC = feKi (ERAND) (7)

Example algorithms for Fe and FX are proposed in [8].

FN: This function takes in a 128 bit ERAND and the secret key Ki as parameter and encrypts a 32 bit RIC to produce a 128 bit output called Encrypted RIC (ERIC).

ERIC=fnKi (RIC; ERAND) (8)

FD: This function decrypts ERIC by using Ki as parameter to produce RIC.

RIC = feKi (ERIC) (9)

Fs: This function stores a freshly generated RIC (RICFresh) against a given IMSI in the HSS's database. In order to make space for RICFresh, the oldest RIC stored against the corresponding IMSI is freed up. For example, for m = 3 with RICNew; RICPrev and RICOld as the RICs stored against the corresponding IMSI, the oldest RIC (i.e., RICOld) is returned to the pool of not-in-use RICs by setting a null pointer against it in the RIC-Index. RICOld is then replaced by

RICPrev, and RICPrev is replaced RICNew. Finally RICNew is replaced by RICFresh. An entry in the RIC-Index against the IMSI-Pointer of RICFresh is also made accordingly.

RICOld: IMSI-Pointer = null (10)

RICOld = RICPrev (11)

RICPrev = RICNew (12)

RICNew = RICFresh (13)

7. IMPLEMENTATION

For implementation purpose I have used

Simulation tool: NS-2.3x

Languages us : C++

Script Languages: AWK, TCL

Graph evaluation: Xgraph

In following module wise:

Module I: Apply LTE patch in ns2 and create a base LTE network with enodeB and users and transfer the data from sender node to receiver node. Implementation: TCL, LTE Patch

Module II: Implement Existing Security architecture model (eNB is connected with one or more Mobility Management Entities (MME) through the S1-MME interface) and transfer data between users and enodeB. Implementation: TCL, C++

Module III: Measure Successful data delivery ratio and delay of Existing Security architecture model implemented LTE network and outputs are shown using graphs. Implementation: TCL, AWK, Xgraph

Module IV: Implement Proposed TRUST MODEL (The UE should trust only the HN with which it is registered and no one else) and transfer data between users and enodeB. Implementation: TCL, C++

Module V: Measure Successful data delivery ratio and delay of Proposed Secure TRUST MODEL implemented LTE network and outputs are shown using graphs. Implementation: TCL, AWK, Xgraph

Module VI: Compare Existing Security architecture model with proposed Secure TRUST MODEL using the measured Parameters (Successful data delivery ratio and delay) and outputs are shown using graphs. Implementation: Xgraph

8. RESULTS

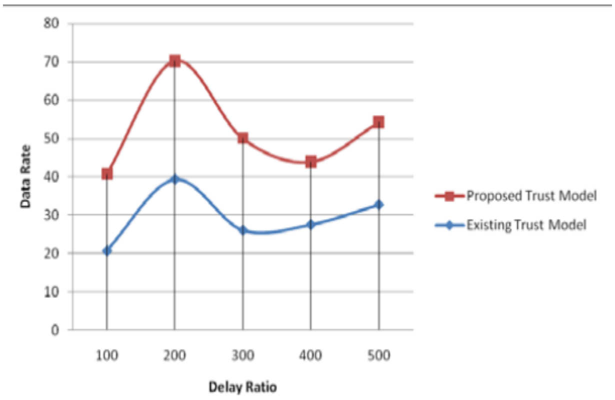

Chart -1: Data Rate vs. Delay Ratio

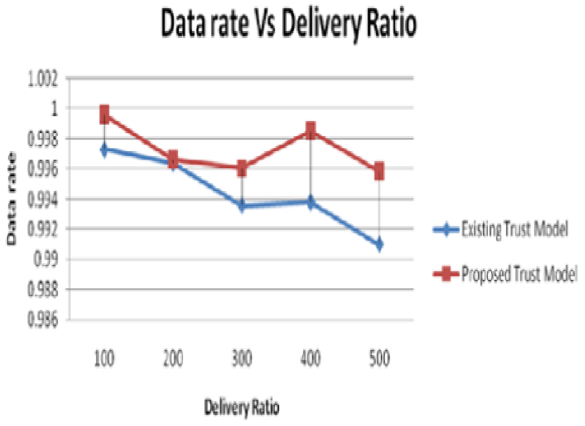

Chart -2: Data rate vs Delivery Ratio

9. CONCLUSIONS

In conclusion, Compare Existing Security architecture model with proposed Secure TRUST MODEL using the measured Parameters (Successful data delivery ratio and delay) and outputs are shown using graphs. As part of conclusion the implementation contributed to understanding the importance and the current status of subscriber's identity privacy in cellular network. With more and more operators taking a plunge into the competitive cellular market, interoperability is a key issue. A major factor that influence the ease at which interoperation may happen between cellular operators, depends on the flexibility of the trust model adopted by a cellular network. This article, implements a trust model that may help in improving the status of identity privacy and as an additional benefit may make interoperability between cellular operators easier. Entire part is considered with reference

REFERENCES

[1] William Stallings, Wireless communications and networking, William Stallings books on computer and data communications technology, Publisher Prentice Hall, 2002, ISBN10 0130408646, ISBN13 9780130408648, Length 584 pages.

[2] 3GPP. 3GPP System Architecture Evolution (SAE); Security architecture. TS 33.401, 3rd Generation Partnership Project (3GPP).

[3] 3GPP. Numbering, addressing and identification. TS 23.003, 3rd Generation Partnership Project (3GPP), 2011Thesis.

[4] M. Zhang and Y. Fang. Security analysis and enhancements of 3gpp authentication and key agreement protocol. Wireless Communications, IEEE Transactions on, 4(2):734–742, 2005.

[5] H. Choudhury, B. Roychoudhury, and D.K. Saikia. Enhancing user identity privacy in lte. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pages 949–957. IEEE, 2012

[6] New Trust Model for Improved Identity Privacy in Cellular Networks at International Journal of Computer Applications (0975 - 8887) Volume 56 - No. 14, October 2012.

[7] 3GPP. General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network. TR 23.401, 3rd Generation Partnership Project (3GPP), 2011.

[8] M. Burrows, M. Abadi, and R.M. Needham. A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 426(1871):233–271, 1989...

[9] G. Wedel and V. Kessler. Formal semantics for authentication logics. In Computer Security ESORICS 96, pages 219–241. Springer, 1996.

[10] 3GPP. 3G Security; Security architecture. TS 33.102, 3rd Generation Partnership Project (3GPP), 2011.

[11] C. Xenakis and L. Merakos. Ipsec-based end-to-end vpn deployment over umts. Computer Communications, 27(17):1693–1708, 2004